Firma Digital

Dirección de Tecnologías de Información Y Comunicaciones

EXPOSITORES:
Msc. Sergio Paz Morales spaz@ccss.sa.cr
Lic. Alekcey Chuprine Díaz achuprid@ccss.sa.cr
Msc. Jose Manuel Zamora Moreira jmzamora@ccss.sa.cr

enda

1. Introducción
2. Estrategias de implementación
3. Uso de tecnologías
4. Demo firma digital
5. Ventajas y beneficios de FD
6. Servicios futuros

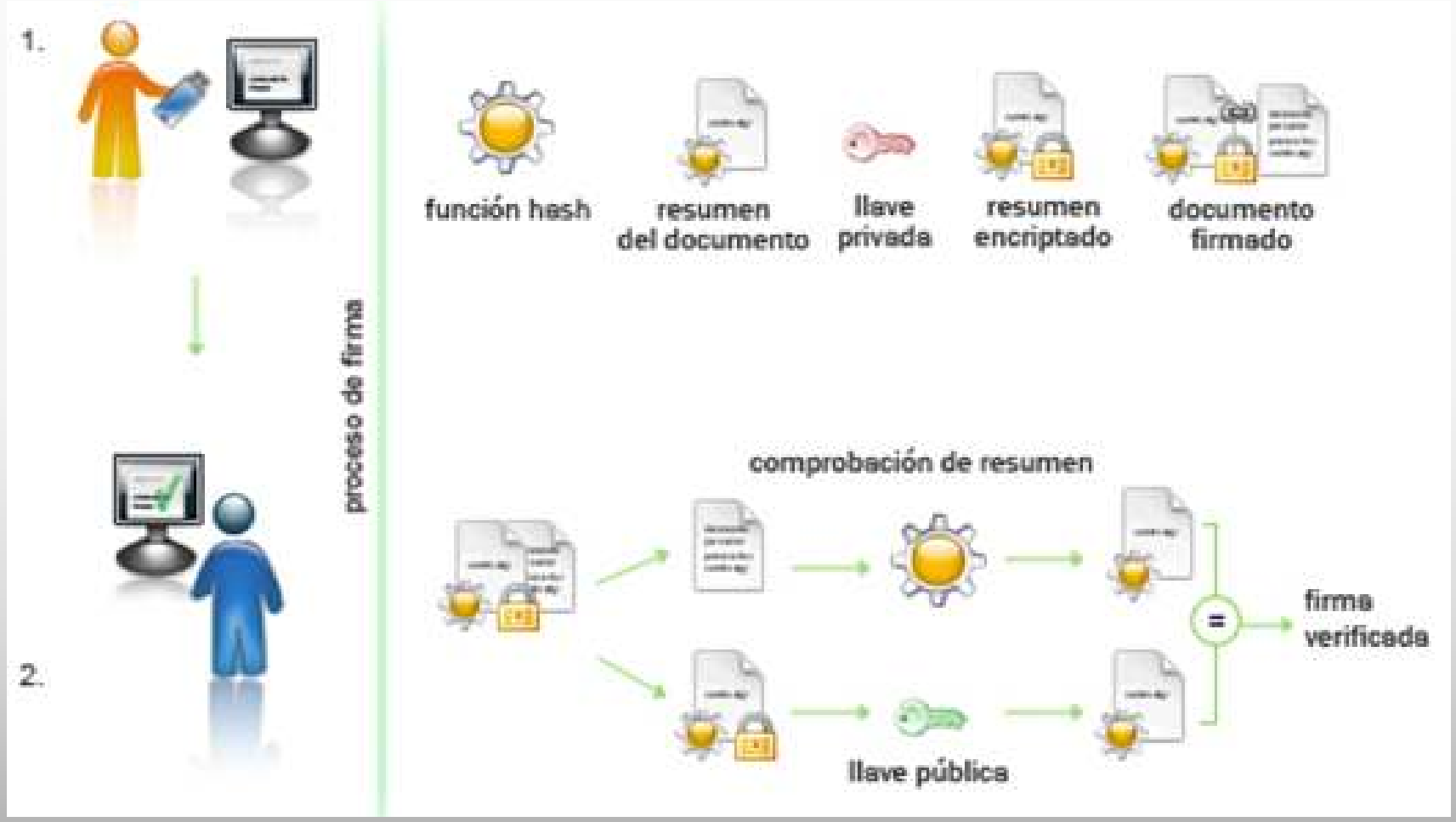
¿Qué es firma digital?

¿Qué se requiere para firmar un documento?

- Certificado digital
- Datos de activación (PIN, huella digital)
- Servicio de validación en línea
- Cadena de confianza

Fuente: sitio oficial de firma digital www.firmadigital.go.cr

Pasos para firmar digitalmente



Fuente: sitio oficial de firma digital www.firmadigital.go.cr

Entidades involucradas en el país

↓

Autoridad Certificadora Raíz

↓

Autoridad Certificadora Emisora

Soporte Firma Digital

Escenarios CCSS

1. Firma de documentos

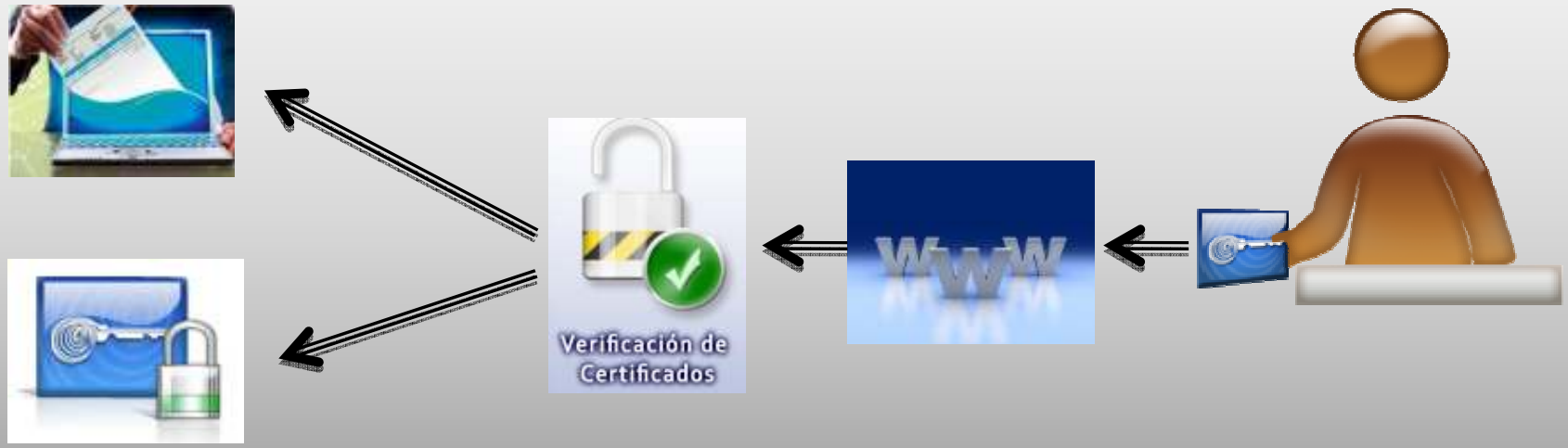
2. Autenticación y autorización en aplicaciones web

Escenarios CCSS

3.Firma de reportes, certificaciones o documentos

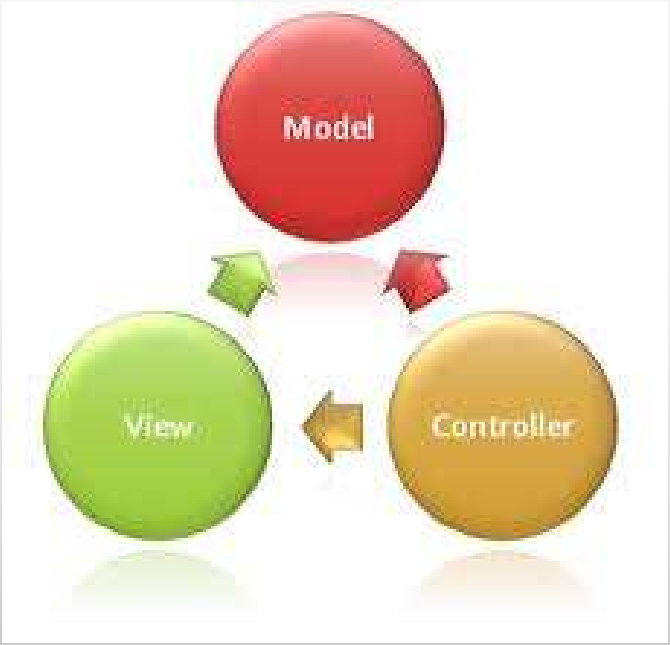
4.Firma de transacciones

5.Validación FD puntos 3 y 4.



Estrategia de implementación

Modelo de arquitectura CCSS



Estrategia de implementación

Portal CCSS

Módulo Admón. FD

Servicios certificado digital

Oficina virtual SICERE

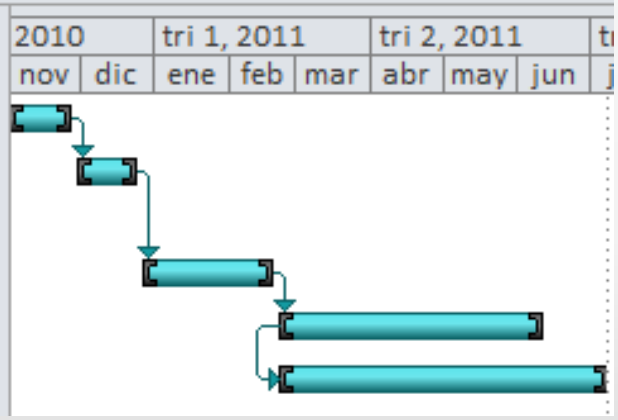
Proveedores

…N

Estrategia de implementación

Plan de trabajo

Nombre de tarea	Duración	Comienzo	Fin
Investigación sobre el tema FD	1 ms	lun 01/11/10	vie 26/11/10
Prueba de concepto autenticación y firma	1 ms	lun 29/11/10	vie 24/12/10
Prototipo funcional FD	2 mss	lun 27/12/10	vie 18/02/11
Desarrollo módulo admón. FD	4 mss	lun 21/02/11	vie 10/06/11
Implementación de servicios	5 mss	lun 21/02/11	vie 08/07/11



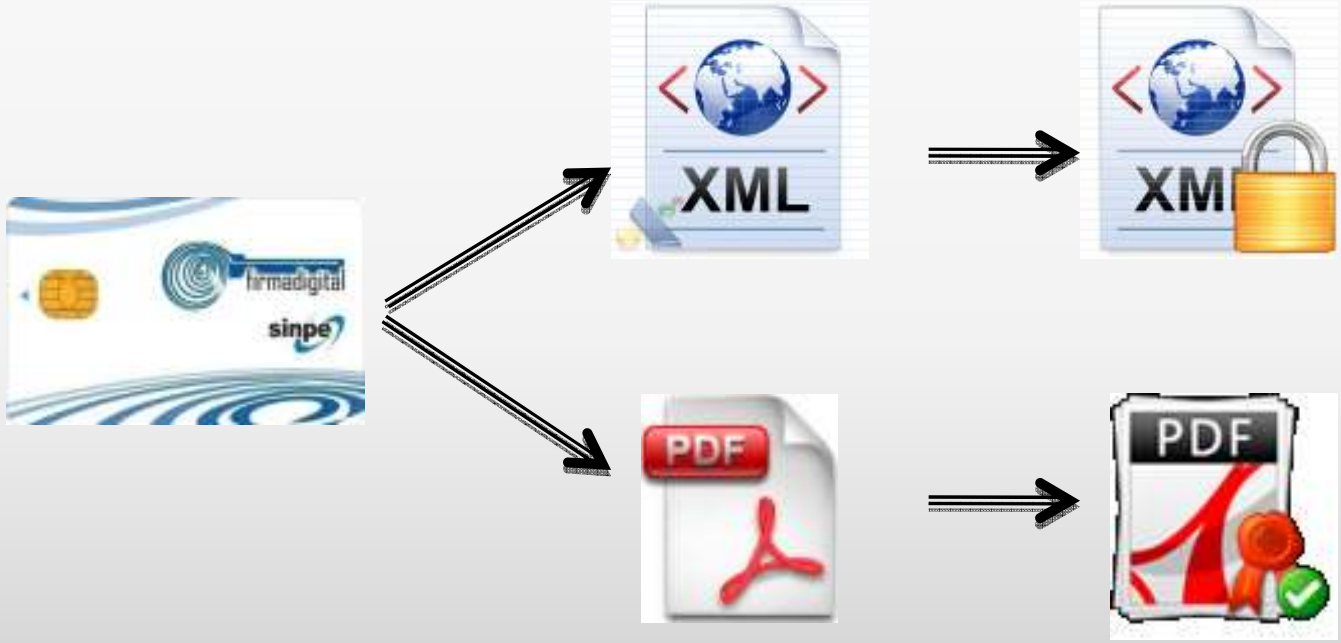
Uso de tecnología de implementación

Crypto

Uso de tecnología de implementación

Navegadores soportados

Demo Firma Digital



Ventajas y beneficios FD

- Disminución de “filas” en Oficinas de la CCSS
- Garantía en uso de mecanismos de seguridad robustos
- Ahorro de Recursos (Papel, impresión, Energía Eléctrica, RRHH)

Ventajas y beneficios FD

- Gestión automatizada (Simplificación de trámites, Gobierno Digital)
- Respaldo Jurídico en la aplicación de la Ley 8454
- Allanar camino en la implementación usuario con “logon único”

Servicios futuros

- Inclusión C.C. RCPI
- Firma de transacciones (estándares país)
- Según requerimientos Usr. Final

MUCH@S GRACIAS!!!

Firma de un texto con Internet Explorer

```
function firmarInternetExplorer(original){
    try{
        // Inicializa los objetos CAPICOM para firmar los datos y atributo de tiempo
        var datosFirmados = new ActiveXObject("CAPICOM.SignedData.1");
        var atributoTiempo = new ActiveXObject("CAPICOM.Attribute.1");
        // Se especifica los datos que se van a firmar
        datosFirmados.Content = suprRetornoCarro(original);
        //datosFirmados.Content = original;
        var Signer = BuscarCertificadoPorHash();
        // Se establece el momento en que se aplico la firma
        var Today = new Date();
        atributoTiempo.Name = CAPICOM_AUTHENTICATED_ATTRIBUTE_SIGNING_TIME;
        atributoTiempo.Value = Today.getVarDate();
        Today = null;
        Signer.AuthenticatedAttributes.Add(atributoTiempo);

        // Se realiza la firma, se codigica con base 64
        var szSignature = datosFirmados.Sign(Signer, true, CAPICOM_ENCODE_BASE64);
        return szSignature;
    }catch (e){
        if (e.number != CAPICOM_E_CANCELLED)
        {
            alert("Hubo un error al momento de realizar la firma: " + e.description);
        }
    }
    return "";
}
```

Firma de un texto con Mozilla FireFox

```
function firmarFirefox(original) {
    //Se llama al paquete crypto que mostrará un cuadro (debido al parametro ask),
    //donde se puede seleccionar el certificado que se va a utilizar, además devuelve el
    //contenido ya firmado, de no ser así se devuelve un error con su causa.
    var firmado = window.crypto.signText(original, "ask");
    //var firmado = window.crypto.signText(original, "auto");
    //Si tuvo un error
    if (firmado.substring(0,5) =="error") {
        alert("Hubo un error al momento de realizar la firma: " + traducirError(firmado));
        return "";
    }
    else if (firmado =="no generada") {
        alert("No ha generado la firma.");
        return "";
    }
    else {
        return firmado ;
    }
}
```

Validación por OCSP

```
boolean resultado = true;
CertificateFactory certFactory = CertificateFactory.getInstance("X.509");
//Se establece las direccion de las cuales se obtendrá el certificado raíz
URL ca_cert = new URL(this.certificadoRaiz);
URLConnection ucCert;
InputStream ccStream;
//Se crea el certificado raíz a partir del stream
X509Certificate certRaiz = (X509Certificate) certFactory.generateCertificate(ccStream);
//Se valida la llave pública entre el certificado del usuario y el ceritificado raíz el BCCR
cert.verify(certRaiz.getPublicKey());
//Se crea el request para el OCSP
OCSPReq request = generateOCSPRequest(certRaiz, cert.getSerialNumber());
//Se codifica el request
byte[] requestCodificado = request.getEncoded();
```

Se consume el request del OCSP

```
//Obtiene la respuesta
InputStream in = (InputStream) con.getContent();
OCSPResp ocspResponse = new OCSPResp(in);
if (ocspResponse.getStatus() != 0){
  resultado = false;
  this.error = ERROR_REVOCADO;
}
```

Manipulación de Datos

```
//Se obtienen los datos personales de la persona que posee el certificado
//Este proceso puede servir para autenticación de personas en los sistemas
if(resultadoValidacion){
    datosPersonales = p7.getCertificates()[0].getSubjectDN().getName();
    if (datosPersonales.lastIndexOf(TIPO_ID)==-1){
        datosPersonales = null;
    }
}
```

```
//Se descompone el String de datos devueltos del certificado y se almacenan en un ArrayList
String [] datosPersonales = idUsuario.split(",");
for (int i = 0; i < datosPersonales.length; i++){
    StringTokenizer tokens = new StringTokenizer(datosPersonales[i], "=");
    tokens.nextToken();
    infoUsuario.add(tokens.nextToken());
}
}
```

Resultado

Nombre Comun	Unidad Organizacional	Organización	País	Nombre	Apellidos	Identificación
ALEKCEY CHUPRINE DIAZ (FIRMA)	CIUDADANO	PERSONA FISICA	CR	ALEKCEY	CHUPRINE DIAZ	CPF-01-1179-0319